Available online at www.sciencedirect.com

ScienceDirect

Journal of Hazardous Materials 159 (2008) 135–141

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

The relationship between automation complexity and operator error

Russell A. Ogle*, Delmar "Trey" Morrison III, Andrew R. Carpenter

Exponent, Inc., 185 Hansen Court, Suite 100, Wood Dale, IL 60134, United States

Received 14 December 2007; accepted 11 January 2008
Available online 31 January 2008

Presented at the 2006 International Symposium, "Beyond Regulatory Compliance: Making Safety Second Nature,"
Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, Texas, October 2006.

Abstract

One of the objectives of process automation is to improve the safety of plant operations. Manual operation, it is often argued, provides too many opportunities for operator error. By this argument, process automation should decrease the risk of accidents caused by operator error. However, some accident theorists have argued that while automation may eliminate some types of operator error, it may create new varieties of error.

In this paper we present six case studies of explosions involving operator error in an automated process facility. Taken together, these accidents resulted in six fatalities, 30 injuries and hundreds of millions of dollars in property damage. The case studies are divided into two categories: low and high automation complexity (three case studies each). The nature of the operator error was dependent on the level of automation complexity. For each case study, we also consider the contribution of the existing engineering controls such as safety instrumented systems (SIS) or safety critical devices (SCD) and explore why they were insufficient to prevent, or mitigate, the severity of the explosion.

Keywords: Process automation; Complexity; Operator error; Case studies

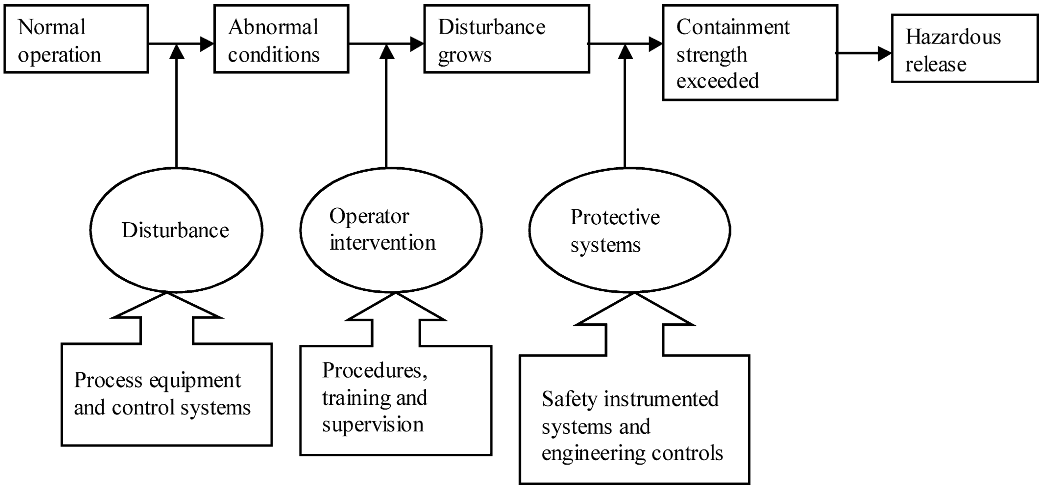
1. Introduction

Several factors are required for the successful operation of chemical process facilities. One of these factors is the control of physical and chemical processes to maintain the desired operational characteristics. The plant operator plays a central role in the control mission. Since the 1960s, there has been a dramatic growth in process automation [1]. This has been stimulated by an interest in both reducing the intensity of manual operation and in increasing the safety of the process by reducing the potential for operator error. But numerous case studies have shown that simply replacing a manual control action with an automated control action does not necessarily reduce the risk of a severe accident [2,3]. Accident prevention requires a balanced analysis of hazards and their control with due consideration of the interactions between the operators, the process equipment, the control systems, and the environment.

A useful accident model for chemical processes is the barrier analysis model [4]. The accident event is a loss of containment of hazardous chemicals or energy. The accident model consists of an initiating event that propagates a disturbance through the system. Operational responses and physical barriers act to reduce (or magnify) the magnitude of the disturbance. The outcome is either success or failure of containment [5,6]. This accident model is illustrated by the figure below.

* Corresponding author.
E-mail address: rogle@exponent.com (R.A. Ogle).

0304-3894/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2008.01.065


Normal operation
Abnormal conditions
Disturbance grows
Containment strength exceeded
Hazardous release
Disturbance
Operator intervention
Protective systems
Process equipment and control systems
Procedures, training and supervision
Safety instrumented systems and engineering controls

Several organizations have published guidelines and standards for safe process automation. For example, the Center for Chemical Process Safety (CCPS), a technical society of the American Institute of Chemical Engineers (AIChE), published a book on safe process automation in 1993 [7]. Following that, the Instrumentation, Systems, and Automation Society (ISA) published a standard for safety instrumented systems (SIS) [8] and the International Electrotechnical Commission (IEC) published their SIS standard in 2003 [9]. These publications address the design, operation, and maintenance requirements for SIS technologies.

AIChE followed these publications with an important contribution to risk assessment involving process automation and safety [6]. This risk assessment methodology, called layer of protection analysis, emphasizes the importance of considering the effectiveness of operator intervention, safety instrumented systems, and engineering controls to prevent or mitigate a hazardous release. Although intended as a semi-quantitative risk assessment methodology, it is also useful as a qualitative accident investigation tool. For a given risk scenario, one must decide how much reliance will be placed on the use of operator intervention, safety instrumented systems, and engineering controls. A qualitative form of layer of protection analysis can assist the accident investigator in evaluating this allocation of safety function.

Too often, facilities rely on operator intervention as their primary line of defense without assessing its potential for success in a given risk scenario. When the risk scenario materializes, the facility may discover that operator intervention may not be successful. When such an accident occurs, it is important to determine if it is the result of simple operator error or if it is indicative of a more systemic deficiency. In this paper we present six case studies of explosions involving operator error in an automated process facility. Taken together, these explosions resulted in six fatalities, 30 injuries and hundreds of millions of dollars in property damage. The case studies are divided into two categories: low and high automation complexity (three case studies each). The nature of the operator error was dependent on the level of automation complexity. We also consider for each case study the contribution of the existing engineering controls such as safety instrumented systems or safety critical devices (SCD) and explore why they were insufficient to either prevent or mitigate the severity of the explosion.

2. Background

The analysis of the accident case studies relies on three characteristics: layer of protection analysis, automation complexity, and operator error.

The layer of protection analysis (LOPA) methodology introduces an important concept helpful for accident investigation: the independent protection layer. The independent protection layer (IPL) is defined as a device, system, or action that is capable of preventing a risk scenario from proceeding to the undesired consequence. IPLs, listed below, follow a natural hierarchy in the order from initiating event to accident outcome:

1. Basic process design.
2. Basic process control system.
3. Critical alarms and operator intervention.
4. Safety instrumented function.
5. Physical protection devices.
6. Post-release physical protection.
7. Plant emergency response.
8. Community emergency response.

Items 1 and 2 are generally not counted as IPLs. For the purposes of accident investigation, we focus our attention on items 3, 4 and 5 with the intent of identifying means for preventing a loss of containment.

Automation complexity refers to the number and connectivity of the information streams that the operator must monitor and maintain. We use it in this study in a qualitative manner:

- Low automation complexity is defined as a situation where the operator is interacting with a single control loop.
- High automation complexity is defined as a situation where the operator is interacting simultaneously with multiple control loops.

More formal (i.e., mathematical) definitions have been suggested using graph-theoretical measures [10]. The qualitative definitions suffice for the purposes of accident investigation.

Operator error is defined here as a deviation from a desired outcome [11]. The accident sequence begins with an initiating event that can be characterized as a process disturbance. The challenge for the operator is to identify, diagnose, and correct the cause of the disturbance. The complex interaction between the human operator, computers and process equipment is thoroughly explored in Nancy Leveson's monograph [12]. A comprehensive discussion of human error issues in the process industries has been published by CCPS [13].

Based on a series of accident investigations conducted by the authors and by others, we gradually developed the hypothesis that in the event of an operator error, the nature of the error was a function of the automation complexity. If automation complexity can influence the type of response or the response time for problem resolution, then some safeguards may be more effective than others in one automation environment versus another.

3. Discussion of case studies

The six case studies are divided into two categories: low and high automation complexity. Table 1 is a summary of the case studies grouped according to automation complexity.

3.1. Low automation complexity

3.1.1. Case 1. Batch process oven

This accident involved an explosion and fireball, which occurred when a flammable atmosphere developed in an oven used to cure machined parts. In this process, batches of machined parts were coated and then cured in large electrical resistance heated ovens. The facility processed a large number of different types of machine parts, with each part requiring slightly different processing conditions. This accident occurred because an operator deviated from the standard operating instructions for this process in an attempt to speed up the process. This accident was further facilitated by the inadvertent modification of the process control system. The resulting explosion and fireball seriously injured two workers and caused significant damage to the facility.

The processing steps and conditions were documented for each machine part in a written standard operating procedure. The part coating process typically required at least four steps: preheating the parts, dip coating, rinsing, and curing. The solvent used for rinsing was naphtha, which had a flashpoint of 106 °F and a lower explosive limit (LEL) of 1.4% at 77 °F.

The oven was a Class B furnace by design, but was installed and operated as a Class A furnace [14]. The oven had a high-limit shut-off, which was set at the oven's maximum design temperature of 650 °F. The oven also had a timer to limit heating duration. The facility implemented administrative controls in the form of a written operating procedure, a specified heating cycle, and an approximate solvent loading. The facility also implemented an engineering safeguard of an external induction fan to purge vapors from the oven in order to remain below the solvent's lower flammable limit. An externally mounted recording temperature controller controlled the oven temperature. A pre-cut plastic cam defined the temperature program. The temperature set-point was controlled by means of a following arm that traveled along the edge of the revolving plastic cam. The radial distance of the follower arm from the hub determined the temperature set-point for the oven. The temperature controller contained a pen that recorded the oven temperature (based on a mercury thermostat) on a circular chart that spun coincident with the temperature cam hub.

In this accident, the operator intentionally disregarded the written procedures by pre-heating the curing oven. The standard cams incorporated a slowly ramped temperature profile, which was thus circumvented by the operator's actions. The operator also inadvertently made the mistake of installing a higher temperature cam, 350 °F, instead of the correct 250 °F cam. The cams were similar in appearance, but were not labeled. The operators typically could identify the temperature setting by the size of the cam. It was undetermined why the operator made the mistake of choosing the higher temperature cam. The coupled intentional and unintentional deviations from the historically safe heating procedure led to a higher than usual concentration of solvent vapors in the already hot oven. These vapors ignited a few minutes into the curing cycle and caused an explosion that ruptured the oven.

This process relied on administrative controls to achieve safe operations. Safe operation required that the operator follow the written procedure. No allowance was made for independent verification by a supervisor that the procedure was being followed. An interlock to prevent oven operation above 250 °F was not feasible as it would limit the utility of the oven. Implementing an engineering control such as using an appropriately designed Class A oven for this application would have prevented this accident.

Table 1
Summary of case studies

Case study	Automation complexity	Automation technology	Safety instrumented system	Operator error	Operator response time
Case 1	Low	Local analog controller	No	Incorrect set-point	1–2 min
Case 2	Low	Manual operation and SCADA/PLC	No	Wrong order of reactant addition	1–2 min
Case 3	Low	Manual operation	No	Limiting reactant omitted	1–2 min
Case 4	High	DCS and SCADA/PLC	Inadequate	Failure to detect abnormal condition	6 h
Case 5	High	SCADA/PLC	Defeated	Failure to detect abnormal condition	4 h
Case 6	High	DCS and SCADA/PLC	Defeated	Wrong control action	30 min

3.1.2. Case 2. Batch polymerization reactor

This accident involved the runaway polymerization of a batch reactor at a polymer resin manufacturing facility. This facility produced many different polymer formulations. The particular mixture that was the subject of this incident was a phenolic resin produced by the reaction of phenol and formaldehyde in the presence of a catalyst. The liquid phase ingredients were added using manually operated valves and the solid ingredients were added by hand. The runaway polymerization was the result of the operator adding the ingredients to the reactor in the wrong order. This accident resulted in one fatality, several injuries, extensive damage to the facility, and the evacuation of portions of the local community.

During the production of this phenolic resin, the reactor vessel was charged with molten phenol, followed by a measured quantity of the catalyst. The formaldehyde solution was then slowly metered into the reactor allowing the reactor to dissipate the heat generated by the polymerization. In this facility, the operator relied on a computerized system that prompted the operator with the steps to complete the batch. The computer acted only as an event recorder and did not have any control function. In this case, the operator charged the reactor with all of the raw materials and the catalyst simultaneously in deviation to the standard operating procedures for this batch. The control system for this operation did not include any interlocks to verify that the prompts generated by the computer system were being followed.

3.1.3. Case 3. Batch hydrogenation reactor

Hydrogen gas was vented through an emergency relief system from a high-pressure hydrogenation reactor and resulted in a large explosion over the facility that caused power outages, structural damage to the facility and nearby residences, and minor injuries to plant personnel. At the time of the incident, the operator was producing a batch of product that involved saturating an organic chemical with hydrogen in the presence of a catalyst. The operator neglected to add the organic component to the mixture, resulting in the vessel being charged with significantly more hydrogen than normal. When the reactor was heated, the internal pressure of the reactor increased causing a rupture disc to function. The quantity of hydrogen vented from the tank was considerably more than the emergency relief system was designed to safely handle. Consequently, the hydrogen cloud ignited over the facility.

During a typical batch, the operator would first charge the reactor with water, and then add the organic phase, followed by the catalyst. The reactor would then be pressurized with hydrogen and heated via internal steam coils. All of the control systems for this process are manual, with the exception of the hydrogen feed. The operator would open and close manual valves to add the liquid components and catalyst into the reactor. The hydrogen feed was manually initiated, but automatically controlled through the internal pressure of the tank. The internal temperature, agitator speed, and pressure would then be monitored during the run to determine when the reaction was complete. During the operation, the pressure would initially fluctuate as hydrogen would react (decreasing the pressure) and make up hydrogen would be added (increasing the pressure). The operator would monitor the rate that hydrogen was being consumed in the reaction and would manually shut-off the hydrogen supply when the rate had decayed to an established level. The pressure would decay as hydrogen reacted with the remaining unsaturated organic phase. Any residual pressure in the reactor would be vented through the emergency relief system.

While the operator monitored the internal temperature and pressure, the system contained no high or low alarms to indicate any unusual operating conditions. The system did not contain any interlocks or controls to ensure if the proper amount of the reactants were added. During the incident run, several times the normal volume of hydrogen was added but the operator had no feedback to indicate to him that there was any unusual condition. Additionally, the operator would look at all of the three outputs on the same screen, so the absolute conditions were not carefully observed, just the trends.

3.2. High automation complexity

3.2.1. Case 4. Batch polymerization reactor II

A vapor cloud explosion occurred at a polyvinyl chloride resin manufacturing plant. Details of the investigation and analysis are contained in Ogle et al. [15]. The explosion originated at an atmospheric storage vessel when it received a slurry discharge from a suspension polymerization reactor. The pressure rise caused by the uncontrolled flashing of superheated liquid vinyl chloride separated the roof from the tank shell causing a release of a cloud of vinyl chloride vapor. The vapor cloud was subsequently ignited resulting in a vapor cloud explosion. The accident caused significant property damage but no serious injuries.

A portion of the polyvinyl chloride (PVC) resin process is depicted in a simplified flow diagram in Fig. 1. The process involved high-pressure, high-temperature reaction of vinyl chloride monomer (VCM) in batch reactors. The process was designed so that reactors could run in a staggered fashion such that one could be emptied while the other was being filled/reacted. The process was monitored and controlled by an operator in a centralized control room via a typical distributed control system with a computerized supervisory control and data acquisition system. The process was highly automated with logic functions being carried out by programmable logic controllers (PLCs) within the control system architecture. Process conditions were monitored through temperature, pressure, and flow rate at strategic locations in the process. The process as originally designed did not contain the degas tank. This vessel was added subsequent to the original design to aid in reactor turnaround between runs by receiving the high-pressure PVC–water slurry, which still contained compressed VCM vapor.

When the degas tank was added, additional instrumentation was not added to monitor pressure or temperature in the discharge tank. Prior to this addition, the reactors were degassed and cooled prior to being transferred through the discharge tank into the slurry tank. After the addition, high-pressure slurry was now introduced into the downstream system between the reactors and the degas tank. Hazard analysis did not reveal the possibil-

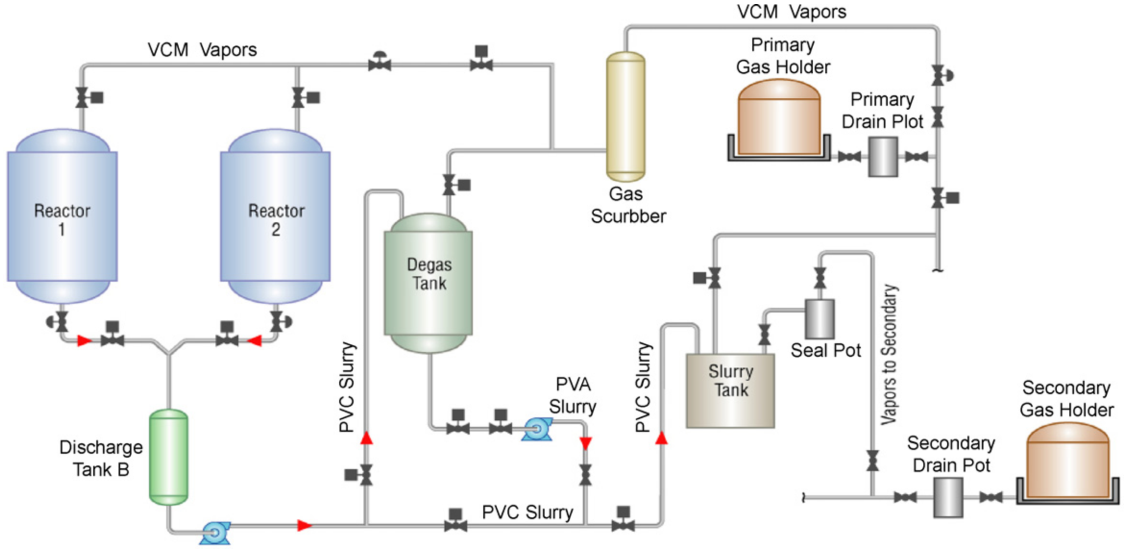


Fig. 1. Polyvinyl chloride slurry synthesis process flow diagram.

ity of trapping high-pressure slurry with condensed VCM in the discharge tank and piping under certain conditions, thus no engineering or administrative controls were administered to protect against it.

The overpressure protection for the slurry tanks was based on a combination of a venting system and a safety instrumentation system. The investigation determined that neither the venting system nor the SIS was adequate to protect the slurry tank from the worst credible overpressure scenario. Fundamentally, this is because the performance objectives of the venting system and SIS were not clearly defined and did not protect against the worst credible overpressure scenario. For example, the SIS included safety interlocks to prevent high-pressure gas from entering the slurry tank through vapor piping, yet did not include interlocks to prevent high-pressure slurry/vapor from entering through the slurry line.

On the day of the accident, both reactors were in operation. Batch 1 was transferred from Reactor 1 to the degas tank and vented there. Reactor 1 remained charged with hot high-pressure VCM vapor, yet sat idle for approximately 2 h while concerns about potential product quality issues delayed processing of Batch 2 in Reactor 2. VCM vapor cooled and condensed in Reactor 1 during this time. High-pressure, condensed VCM was then transferred with wash water from Reactor 1 into the discharge tank. Eventually the quality issues with Batch 2 were resolved and Reactor 2 was vented directly. The next step was to transfer the hot slurry from Batch 2 to the slurry tank. Shortly after the operator opened the automatic block valve from the operator interface to begin the transfer, the slurry tank ruptured due to the introduction of the hot slurry into the cool, condensed VCM in the discharge tank.

3.2.2. *Case 5. Ethylene oxide sterilization process explosion*

The U.S. Chemical Safety and Hazard Investigation Board (CSB) investigated an accident involving an explosion of an ethylene oxide sterilization process and its associated air pollution control system [16]. The facility uses a series of batch reactor chambers to sterilize pallets of boxed medical products by prolonged exposure to ethylene oxide (EO) gas (see Fig. 2). An individual reactor chamber is loaded with the products then sealed. The sterilization cycle consists of drawing an initial vacuum, dwelling under EO atmosphere, vacuum purging, nitrogen/air pressure purging, then sweep-through purging with air. During the sterilization dwell, the chamber is maintained at slightly sub-atmospheric pressure with approximately 40% by volume EO. The flammable range for EO is 2.6–100% by volume. In addition to flammability hazards, EO presents a toxic exposure hazard. The exhaust gases from the pressure purge were rich in EO and thus sent to a chemical scrubber. After pressure purging, the chamber door was raised slightly causing a vent interlock to open allowing the exhaust to vent to the catalytic oxidizer. The system was designed so that the concentration of EO should remain under 25% of the lower explosion limits (LEL) in the exhaust to the catalytic oxidizer. Higher concentrations present the hazard of ignition of the fuel air mixture. EO flame fronts spread fast enough that typical explosion prevention measures in the vent line would not be suitable.

The operation of the process was automated through a computerized control system. The system was recipe driven, such that an operator entered the recipe, then the batch sterilization cycle advanced through each of the steps as per the process design. This automatic system could be circumvented and taken under manual control through the use of an administrator password by a supervisor. The control system monitored pressure of the chamber only. It did not measure the concentration of EO; thus provided no safety oversight for preventing the accumulation of a flammable mixture in the chamber.

Prior to the accident, a sterilization cycle had to be aborted due to an EO injection failure. After that batch was aborted, the maintenance staff worked on the empty chamber. The maintenance personnel performed an abbreviated 4 lb EO injection cycle. After that cycle was completed satisfactorily, they ran a calibration cycle that used 125 lbs of EO. After this injec-

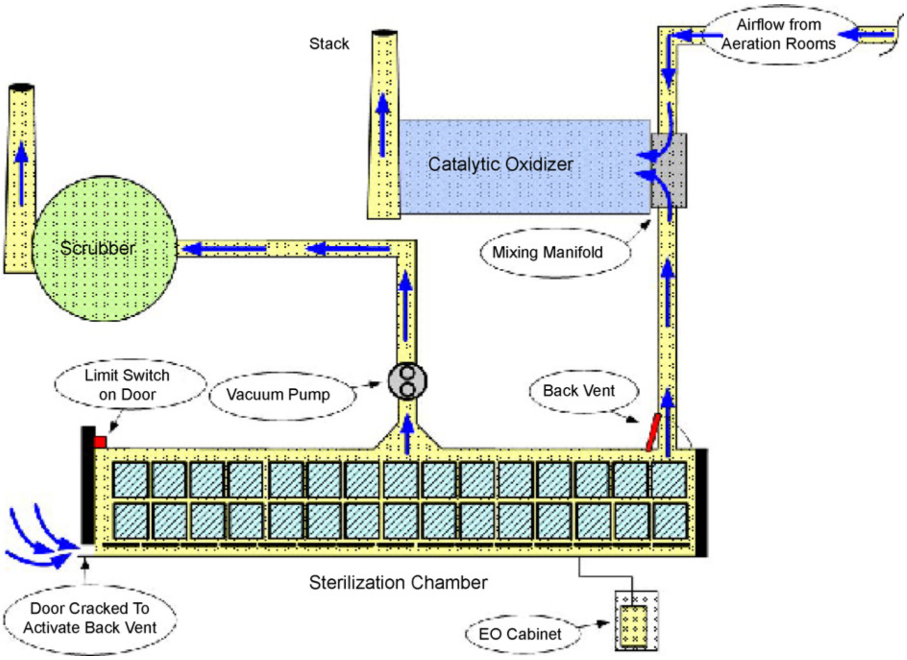


Fig. 2. Ethylene oxide sterilization process [16].

tion cycle was completed satisfactorily, the technicians received approval from the maintenance supervisor (and the password) to skip the pressure purging and advance directly to the manual action of sweep-through purging. The technician opened the chamber door to initiate venting to the catalytic oxidizer. Shortly thereafter, LEL alarms in the chamber room activated, signaling the release of EO from the oven. The EO–air mixture was subsequently ignited before the oxidizer could be shut down. The CSB estimated that 50 lbs of EO remained in the chamber at the start of venting. The explosion destroyed the chamber, caused one injury, and caused significant property damage.

Among the CSB's findings, the control system was deficient because there was no direct measure of either LEL or concentration of EO in the chamber. Also, password bypass of the existing safety interlocks was not carefully administered. There is also an indicator that external LEL alarms were not interlocked with the catalytic oxidizer to shut it down or isolate it from the chambers.

3.2.3. Case 6. Continuous mineral processing facility

A large chemical plant explosion occurred in a mineral processing facility. The facility was approximately 40 years old and used a process of high temperature and pressure liquid extraction to separate desired material from ore. The high-pressure process stream was passed through a series of flash tanks to reduce the pressure and temperature to atmospheric levels. The explosion occurred in the flash tank section of the extraction plant and resulted in the total destruction of that area, widespread plant damage, and several injuries.

During the early morning hours on the day of the accident, the shift change was occurring normally until the plant suffered an electrical power outage. The operator for the high-pressure extraction unit initiated emergency shutdown. The extraction unit had not been fully shutdown for several years except in the case of complete utility outages (i.e., both electrical and steam). The emergency relief system was undergoing maintenance and was partially disabled. The unit had a computerized supervisory control and data acquisition (SCADA) system in parallel with an analog control panel integrated with DCS to monitor pressure and liquid levels in the reactor vessels and flash vessels. The operators typically interacted with the analog controllers on the control panel as opposed to the computerized system to implement control actions. The DCS also monitored reactant feeds. Among these were crushed ore, recycled process liquor, and superheated steam, which were injected into the reactor vessels at the front end of the process.

Several minutes into shutdown of the high-pressure extraction unit, there was a catastrophic explosion in the unit. Half of the flash vessels in the unit exploded; the resulting debris, piping, equipment, and pressure vessel fragments were thrown up to 2/3 of a mile from the unit. Several employees were injured during the catastrophic failure from flying debris, steam, and boiling process liquor.

From the witness interviews and process data, it was determined that 6 months prior to the explosion the plant had experienced a similar emergency shutdown due to a total utility outage without incident. The differences between these two shutdowns were evaluated to determine which of these could be root causes for the explosion. The unit did not have a written shutdown plan or an automated shutdown function in the SCADA system. The operator responded in a similar fashion to past total utility outage operator responses by opening the reactor discharge valves fully to allow the reactors to “blow down.” In this situation, where superheated steam was still online but liquor and ore moving machinery was offline, those actions proved to be incorrect because the steam further pressurized the reactor vessels and accelerated the slurry discharge beyond levels previously experienced.

The measurement ranges for the analog controllers and chart recorders were exceeded for many of the flash tanks early in the upset. The operator disregarded this result and focused instead on the pressure trends in downstream flash tanks, which were still in range. Unfortunately, the pressure ranges for the instruments were not proportionally aligned with the strength of the vessels and piping. Thus, the upstream vessels failed before the downstream pressures ran off chart.

There was not an interlock in place to isolate the superheated steam supply if the liquor pumps and ore conveyors failed. Although the pressure relief system was partially disengaged, its presence may not have mitigated the mechanical effects of the uncontrolled "blow down." The additional pressure drop may have exacerbated the mechanical forces on the system subsequently leading to a similar failure.

4. Insights from layer of protection analysis

Some valuable insights can be derived from these case studies using layer of protection analysis. First, in four of the six case studies the very accident that occurred had been predicted in a process hazard analysis (PHA). In these PHAs, the effectiveness of operator intervention had been greatly overestimated. Second, in each case a relatively simple safety instrumented system could have reduced the probability, or perhaps prevented the accident.

In the low automation complexity environments the operator errors tended to be simple lapses (unintentional action). The response time for problem identification, diagnosis and correction was typically less than 2 min. This placed an enormous time pressure on successful operator intervention. In each of these three cases, the operator was aware that there was a problem but was unable to successfully intervene. These case studies suggest that high hazard processes with low automation complexity may benefit greatly from a simple safety instrumented system.

In the high automation complexity environments, the operator errors were intentional but mistaken actions. The response time for problem identification, diagnosis and correction ranged from 30 min to 6 h. In these cases it would seem that operator intervention could have been successful if the necessary data and alarms had been available. In each of these three cases the operator failed to detect the abnormal condition. Alternatively, an effective safety instrumented system could have greatly reduced the probability of the accident.

All other things being equal, a low complexity automation environment (e.g., a single control loop) will have a relatively short response time. This short response time has the potential to place an enormous burden on the operator during an emergency. If operator intervention is the preferred safeguard for controlling the emergency, then the procedure must be simple and well rehearsed. If there is insufficient time for operator intervention, then a safety instrumented system may be a better alternative.

Complex automation environments (e.g., multiple, interacting control loops) will have relatively longer response times. This longer response time can increase the probability of success for operator intervention. However, successful operator intervention requires that the operator has both adequate process measurement data and a correct mental model of the process. Otherwise he will not be able to diagnose and correct the cause of the process upset.

5. Conclusions

Abnormal operating conditions can pose a serious threat to the safe operation of chemical processes. Successful prevention or mitigation of a loss of containment requires a careful and effective allocation of the safety function among operator intervention, safety instrumented systems, and engineering controls. The operator is central to the control mission. To effectively intervene and mitigate a process disturbance, the operator must have the information needed to diagnose the problem, must receive the information with adequate time to respond, and must have the appropriate skills and knowledge to implement the corrective action.

References

[1] D.E. Noble, Forces of Production: A Social History of Industrial Automation, Oxford University Press, 1984, pp. 59–66.

[2] T. Kletz, P. Chung, E. Broomfield, C. Shen-Orr, Computer Control and Human Error, Gulf Publishing, 1995.

[3] HSE, Out of Control: Why Control Systems Go Wrong and How to Prevent Failure, Health & Safety Executive, 2003.

[4] P.F. Wilson, L.D. Dell, G.F. Anderson, Root Cause Analysis: A Tool for Total Quality Management, ASQC Quality Press, 1993, pp.131–150.

[5] J. Reason, Managing the Risks of Organizational Accidents, Ashgate Publishing, 1997.

[6] CCPS, Layer of Protection Analysis: Simplified Process Risk Assessment, American Institute of Chemical Engineers, Center for Chemical Process Safety, 2001.

[7] CCPS, Guidelines for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, Center for Chemical Process Safety, 1993.

[8] ANSI/ISA S.84.01, Application of Safety Instrumented Systems for the Process Industries, The Instrumentation, Systems and Automation Society, 1996.

[9] IEC, IEC 61511 Functional Safety: Safety Instrumented Systems for the Process Sector, International Electrotechnical Commission, Geneva, Switzerland, 2003.

[10] J.J. Sammarco, A normal accident theory-based complexity assessment methodology for safety-related embedded computer systems, PhD Dissertation, West Virginia University, 2003.

[11] J. Reason, Human Error, Cambridge University Press, 1990.

[12] N.G. Leveson, Safeware: System Safety and Computers, Addison Wesley, 1995.

[13] CCPS, Guidelines for Preventing Human Error in Process Safety, American Institute of Chemical Engineers, Center for Chemical Process Safety, 1994.

[14] NFPA 86: Standard for Ovens and Furnaces, National Fire Protection Association, Quincy, Massachusetts, 2003.

[15] R.A. Ogle, M.V. Megerle, D.R. Morrison, A.R. Carpenter, Explosion caused by flashing liquid in a process vessel, J. Hazard. Mater. 115 (2004) 133–140.

[16] Investigation Report: Sterigenics, U.S. Chemical Safety and Hazard Investigation Board (CSB), Washington DC, 2004.